Journal of Number Theory **73**, 182–194 (1998)
Article No. NT982291

Real Quadratic Fields with Abelian 2-Class Field Tower

Elliot Benjamin

Department of Mathematics, Unity College, Unity, Maine 04988

Franz Lemmermeyer

Fachbereich Mathematik, Universität des Saarlandes, D-66041 Saarbrücken, Germany

and

C. Snyder

Communicated by M. Pohst

Received June 5, 1996; revised February 18, 1998

We determine all real quadratic number fields with 2-class field tower of length at most 1. © 1998 Academic Press

1. INTRODUCTION

Let k be a real quadratic number field. Golod and Shafarevic (cf. [7 and 15]) have shown that k has an infinite 2-class field tower if the 2-rank of $\mathrm{Cl}_2(k)$ is $\geqslant 6$. Martinet ([15]) and Schoof ([19]) have given examples of quadratic fields with infinite 2-class field tower whose 2-class groups have smaller rank, but the following problem remains unsolved:

Problem 1. Determine the smallest integer t such that the 2-class field tower of every real quadratic number field whose class group has 2-rank $\geqslant t$ is infinite.

Since it is easy to give examples of fields with finite 2-class field tower and rank $\mathrm{Cl}_2(k) = 3$, we conclude that $4 \leqslant t \leqslant 6$.

The smallest known example of a real quadratic field with infinite 2-class field tower is due to Martinet, who showed that $\mathbb{Q}(\sqrt{3 \cdot 5 \cdot 13 \cdot 29 \cdot 61})$ has infinite 2-class field tower. The Odlyzko bounds (under the assumption of the Generalized Riemann Hypothesis) show that any real quadratic

0022-314X/98 $25.00

number field with infinite 2-class field tower must have discriminant >46356. This means that the following problem could be solved by a finite amount of computation if we only knew how to decide whether a given number field has finite or infinite 2-class field tower:

Problem 2. Determine the smallest discriminant $d>0$ of a quadratic number field such that $\mathbb{Q}(\sqrt{d})$ has infinite 2-class field tower.

In this paper we determine all real quadratic number fields with abelian 2-class field towers, thus sorting out those fields which are "uninteresting" with regard to Problem 2. The classification makes use of quite a few results in algebraic number theory, for example the class number formula for V_4-extensions, results on unramified 2-extensions of quadratic number fields, the behavior of units in multiquadratic extensions, and Schur multipliers.

2. NOTATION AND PRELIMINARIES

Let k be an algebraic number field with ideal class group in the wide sense, respectively narrow sense, denoted by $\mathrm{Cl}(k)$ and $\mathrm{Cl}^+(k)$. We denote the 2-class groups, i.e. the Sylow 2-subgroup of these groups, by $\mathrm{Cl}_2(k)$ and $\mathrm{Cl}_2^+(k)$. Let $h(k)$ and $h_2(k)$ denote the class number and 2-class number of k, respectively. Also let E_k denote the unit group of $\mathcal{O}_k$, the ring of integers of k We denote by $k^{(1)}$ the Hilbert 2-class field of k, i.e. the maximal abelian unramified (including all infinite primes) extension K/k of degree a power of 2. Likewise, the second Hilbert 2-class field of k, denoted $k^{(2)}$, is the field $(k^{(1)})^{(1)}$.

If k is a real quadratic number field with discriminant $d=\operatorname{disc} k$, the maximal subfield k_{gen} of $k^{(1)}$ which is abelian over $\mathbb{Q}$ is called the genus field of k. If the discriminant $d=d_1 \cdots d_t$ is a product of prime discriminants d_j, then we have $k_{\text{gen}}=\mathbb{Q}(\sqrt{d_1}, ..., \sqrt{d_t}) \cap \mathbb{R}$.

We shall also need to consider the maximal abelian 2-extension of k which is unramified at the finite primes. This field is called the extended Hilbert 2-class field and is denoted by $k^{+(1)}$. Similar remarks apply to $k^{+(2)}$ and k^+_{gen}. We then have $k^+_{\text{gen}}=\mathbb{Q}(\sqrt{d_1}, ..., \sqrt{d_t})$.

We shall need a few results of Scholz, Rédei and Reichardt on the 2-class group of real quadratic number fields, for proofs, we refer to [16, 17, and 18]. D_4 denotes the dihedral group of order 8. Moreover, (d/p) is the Kronecker symbol, which is defined in the usual way to describe the decomposition of the prime p in the quadratic field with discriminant d, and extended by multiplicativity to all integers in the denominator using $(d/-1)=1$. Also $(\cdot/\cdot)_4$ is the rational biquadratic residue symbol, and

$(d/8)_4$ is defined to be $+1$ for discriminants $d \equiv 1 \bmod 16$ and -1 for $d \equiv 9 \bmod 16$. A G-extension K/k is a normal extension with Galois group $G = \mathrm{Gal}(K/k)$. The next two propositions provide criteria for the existence of unramified G-extensions of quadratic number fields for the cyclic group C_4 of order 4 and the quaternion group H_8 of order 8:

PROPOSITION 1. *Let k be a quadratic number field with discriminant d. There exists a C_4-extension L/k which is unramified at all finite primes if and only if there is a factorization $d = d_1 d_2$ into two relatively prime discriminants such that $(d_1/p_2) = (d_2/p_1) = 1$ for all primes $p_i \mid d_i$. In this case, L is normal over $\mathbb{Q}$ with* $\mathrm{Gal}(L/\mathbb{Q}) \simeq D_4$.

If d is a sum of two squares, then L is real if and only if

$$(d_1/d_2)_4 = (d_2/d_1)_4. \tag{1}$$

COROLLARY 1. *Let k be a real quadratic number field. If $F \neq k$ is a real quadratic extension of $\mathbb{Q}$ contained in k_{gen}, and if* $\mathrm{Cl}(F)$ *has a cyclic subgroup of order* 4, *then $k^{(2)} \neq k^{(1)}$.*

Proof. Let $F \subseteq k_{\mathrm{gen}}$ be a real quadratic number field such that $\mathrm{Cl}(F)$ has a cyclic subgroup of order 4. Then there exists an unramified cyclic quartic extension L/F; hence $\mathrm{Gal}(L/\mathbb{Q}) \simeq D_4$ by Proposition 1. But then kL/k is an unramified extension with Galois group isomorphic to D_4 by the translation theorem of Galois theory. Thus the corollary. ∎

These results have a counterpart for unramified quaternion extensions of quadratic number fields [14]:

PROPOSITION 2. *Let k be a quadratic number field with discriminant d. There exists an H_8-extension L/k which is unramified at all finite primes and normal over $\mathbb{Q}$ if and only if there is a factorization $d = d_1 d_2 d_3$ into three relatively prime discriminants such that $(d_1 d_2/p_3) = (d_2 d_3/p_1) = (d_3 d_1/p_2) = 1$ for all primes $p_i \mid d_i$.*

If d is a sum of two squares, then L is real if and only if

$$\left(\frac{d_1 d_2}{d_3}\right)_4 \left(\frac{d_2 d_3}{d_1}\right)_4 \left(\frac{d_1 d_3}{d_2}\right)_4 = \left(\frac{d_1}{d_2}\right)\left(\frac{d_2}{d_3}\right)\left(\frac{d_3}{d_1}\right). \tag{2}$$

We also need the following proposition, which collects results about units (cf. [1, 12]); the genus characters used below are defined as follows: let $d = d_1 \cdots d_t$ be the factorization of $d = \operatorname{disc} k$ into prime discriminants, and let $a > 0$ be the norm of a prime ideal. Then $\chi_i(a) = (d_i/a)$ if $(d_i, a) = 1$, and $\chi_i(a) = (d_i'/a)$ otherwise, where $d_i' = d/d_i$; now extend χ_i multiplicatively to all ideal norms a.

PROPOSITION 3. *Let $k=\mathbb{Q}(\sqrt{m})$ be a real quadratic number field, and assume that m is square-free. Suppose moreover that the fundamental unit ε of $\mathcal{O}_k$ has norm $+1$. Then there exists a principal ideal $\mathfrak{a}=(\alpha)$ which is different from (1) and $(\sqrt{m})$ and which is the product of pairwise distinct ramified prime ideals.*

Moreover, $k(\sqrt{\varepsilon})=k(\sqrt{\delta})$, where $\delta=\delta(\varepsilon)=N_{k/\mathbb{Q}}\alpha$. Finally, we have $\chi_i(\delta)=+1$ for all genus characters χ_i in k.

Remark. If $\mathfrak{a}$ is such an ideal, then so is $2(\sqrt{m})\,\mathfrak{a}^{-1}$ or $(\sqrt{m})\,\mathfrak{a}^{-1}$ (depending on whether $d\equiv 4 \bmod 8$ and $2\mid N\mathfrak{a}$ or not). Similarly, there are two choices for δ, corresponding to the square-free kernels of $N(\varepsilon+1)$ and $N(\varepsilon-1)$ (see [12]). Note, however, that the extension $k(\sqrt{\delta})$ is well-defined; moreover, the image of δ in $\mathbb{Q}^\times/\mathbb{Q}^\times\cap k^{\times 2}$ is uniquely determined.

Proof. Since $N\varepsilon=+1$, Hilbert's theorem 90 shows that $\varepsilon=\alpha^{1-\sigma}$ for some $\alpha\in\mathcal{O}_k$. (Here σ is the nontrivial automorphism on k.) Then (α) is an ambiguous ideal, and by making α primitive (i.e. by cancelling all rational integer factors) we may assume that $\mathfrak{a}=(\alpha)$ is the product of pairwise different ramified prime ideals. Moreover, we clearly have $(\alpha)\neq(1), (\sqrt{m})$.

Now from $\varepsilon=\alpha^{1-\sigma}$ we get that $\varepsilon\delta=\alpha^{1-\sigma}\alpha^{1+\sigma}=\alpha^2$ is a square in k, so $\sqrt{\varepsilon}$ and $\sqrt{\delta}$ generate the same quadratic extension. Next, since $\varepsilon=(\varepsilon+1)^{1-\sigma}$, we can take δ to be the square-free kernel of $N(\varepsilon+1)$. Finally, since α has positive norm, the ideal (α) is principal in the strict sense, and in particular, it lies in the principal genus. This implies our last claim (cf. [21]). ∎

Since our goal is to determine all real quadratic number fields with abelian 2-class field tower, the following result will simplify our work considerably.

PROPOSITION 4. *Let k be a number field, and let r denote the p-rank of E_k/E_k^p. If the p-class field tower of k is abelian, then $\operatorname{rank} \mathrm{Cl}_p(k)\leqslant(1+\sqrt{1+8r})/2$.*

Proof. Assume that the p-class field tower terminates at $K=k^{(1)}$. Then by [8] the Schur Multiplier of $\mathrm{Gal}(K/k)$, $\mathcal{M}(\mathrm{Gal}(K/k))\simeq E_k/N_{K/k}E_K$. This implies that $\mathcal{M}$ has p-rank at most r. On the other hand, the p-rank of $\mathcal{M}$ is just $\binom{s}{2}$, where s denotes the p-rank of $\mathrm{Cl}_p(k)$. (This is a result of Schur (cf. [10], Corollary 2.2.12).) Now $s(s-1)/2\leqslant r\Leftrightarrow(2s-1)^2\leqslant 1+8r$, and taking the square root yields our claim. ∎

This result is originally due to, Bond (see [3], where a different proof is given). In the special case of real quadratic fields and $p=2$ it implies

COROLLARY 2. *Suppose k is a real quadratic field such that $k^{(1)} = k^{(2)}$. Then the 2-rank of* $\mathrm{Cl}(k)$ *is* $\leqslant 2$.

The following class number formula (see [12]) will be applied repeatedly in our proof:

PROPOSITION 5. *Let K be a real bicyclic biquadratic extension of $\mathbb{Q}$ with quadratic subfields k_1, k_2 and k_3. Let E_K, E_1, E_2, E_3 denote their unit groups. Then $q(K) = (E_K : E_1 E_2 E_3)$ is an integer dividing 4, and we have $h(K) = (1/4)\, q(K)\, h(k_1)\, h(k_2)\, h(k_3)$.*

Our last ingredient is an elementary remark on central class fields:

PROPOSITION 6. *Let K/k be a finite p-extension of number fields. If $h(K)$ is divisible by p, then $K_{\mathrm{cen}} \neq K$. Here, K_{cen} denotes the maximal finite unramified p-extension L/K such that L/k is normal and* $\mathrm{Gal}(L/K) \subseteq Z(\mathrm{Gal}(L/k))$, *the center of* $\mathrm{Gal}(L/k)$.)

Proof. This follows from the well-known fact ([13]) that finite p-groups have nontrivial center; see [5, 6 or 20] for more on central class field extensions. ∎

3. THE CLASSIFICATION

If k has trivial or cyclic 2-class group, then the 2-class field tower terminates at $k^{(1)}$. Since the classification of these fields is well known, we only consider the remaining case where

$$\mathrm{Cl}_2(k) \simeq (2^m, 2^n)$$

for m, n positive integers. (Here $(a_1, ..., a_t)$ means the direct product of cyclic groups of orders $a_1, ..., a_t$.)

In light of Corollary 2 above, we consider real quadratic number fields k with 2-class group of type $(2^m, 2^n)$ for $m, n > 0$. By genus theory we know that if $\mathrm{Cl}_2(k)$ is of this type, then the discriminant of k is a product of three positive prime discriminants or a product of four prime discriminants, not all of which are positive. We shall split the work into two cases according as the discriminant of k is a sum of two squares or not. (Recall that the discriminant is a sum of two squares if and only if it is a product of positive prime discriminants.) But before we consider these cases, we state and prove the following general proposition.

PROPOSITION 7. *Let k be a number field with* $\mathrm{Cl}_2(k) \simeq (2^m, 2^n)$ *and $m, n > 0$. If there is an unramified quadratic extension of k with 2-class* *number 2^{m+n-1}, then all three unramified quadratic extensions of k have 2-class number 2^{m+n-1}, and the 2-class field tower of k terminates at $k^{(1)}$. Conversely, if the 2-class field tower of k terminates at $k^{(1)}$, then all three unramified quadratic extensions of k have 2-class number 2^{m+n-1}.*

Proof. Suppose that $K = k^{(1)}$ has even class number. Then the central class field K_{cen} of K/k is not trivial by Proposition 6. Let $L \subseteq K_{\text{cen}}$ be a quadratic extension of K. Now L/k is normal, so let $\Gamma = \text{Gal}(L/k)$ denote its Galois group. Then Γ is a 2-group of order 2^{m+n+1} such that $\Gamma' \simeq \mathbb{Z}/2\mathbb{Z}$ and $\Gamma/\Gamma' \simeq (2^m, 2^n)$. This implies that Γ is generated by two elements σ, τ such that $\Gamma' = \langle [\sigma, \tau] \rangle$. Notice that Γ contains three subgroups Γ_i of index 2. They are $\Gamma_1 = \langle \sigma^2, \tau, \Gamma' \rangle$, $\Gamma_2 = \langle \sigma, \tau^2, \Gamma' \rangle$, and $\Gamma_3 = \langle \sigma^2, \sigma\tau, \tau^2, \Gamma' \rangle$. Their commutator subgroups can easily be computed: it turns out that $\Gamma_i' = 1$ for $i = 1, 2, 3$ (observe, for example, that $[\sigma, \tau^2] = [\sigma, \tau]^2 = 1$ since Γ' is contained in the center of Γ): therefore $\Gamma_i' = 1$, i.e. all subgroups of index 2 are abelian.

But now each Γ_i fixes a quadratic extension K_i of k, and L/K_i is an unramified abelian extension. This implies that the class numbers of the K_i are divisible by 2^{m+n}, contradicting our assumptions.

Therefore $k^{(1)}$ has odd class number, and the ideal class groups of the K_i correspond to the three subgroups of index 2 in $(2^m, 2^n)$.

The converse is almost trivial: if $k^{(1)}$ has odd class number, it is the Hilbert 2-class field of every intermediate field N/k of $k^{(1)}/k$; class field theory then shows that N has 2-class number $(k^{(1)} : N)$. Now apply this to the three quadratic unramified extensions of k. ∎

Case 1. d is a Sum of Two Squares.

PROPOSITION 8. *Let $d = d_k = d_1 d_2 d_3$, where the d_j are prime discriminants, be a sum of two squares, and suppose that the fundamental unit ε of k has norm $+1$. Then $k^{(1)} \neq k^{(2)}$.*

Proof. By Proposition 3, the fundamental unit ε becomes a square in one of the extensions $k(\sqrt{d_i})$ (without loss of generality since $k(\sqrt{d_i}) = k(\sqrt{d/d_i})$); call it M. Then this shows that $q(M) \geqslant 2$. Applying the class number formula (Proposition 5) to $M/\mathbb{Q}$ gives $h_2(M) = (1/4)\, q(M)\, h_2(k)\, h_2(\mathbb{Q}(\sqrt{d/d_i}))$; since both $q(M)$ and the class number of $\mathbb{Q}(\sqrt{d/d_i})$ are even, we find that M has 2-class number divisible by $h_2(k)$. Since M/k is an unramified quadratic extension with $h_2(k)$ dividing $h_2(M)$, Proposition 7 (the converse direction) implies $k^{(1)} \neq k^{(2)}$. ∎

We are now ready to state and prove our first theorem.

THEOREM 1. *Let k be a real quadratic number field with $d_k = d = d_1 d_2 d_3$, where d_j are prime discriminants divisible by the primes p_j and such that*

$d_j > 0$. *Then the 2-class field tower terminates at* $k^{(1)}$ *if and only if the* d_j *have one of the following properties*:

1. $(d_1/d_2) = (d_2/d_3) = (d_3/d_1) = -1$, $(d_1 d_2/d_3)_4 \, (d_2 d_3/d_1)_4 \, (d_3 d_1/d_2)_4 = +1$;
2. $(d_1/d_2) = +1$, $(d_2/d_3) = (d_3/d_1) = -1$, $(d_1/d_2)_4 \, (d_2/d_1)_4 = -1$;
3. $(d_1/d_2) = (d_2/d_3) = +1$, $(d_3/d_1) = -1$, $(d_1/d_2)_4 \, (d_2/d_1)_4 = (d_2/d_3)_4 (d_3/d_2)_4 = -1$ *and* $N\varepsilon = -1$;
4. $(d_1/d_2) = (d_2/d_3) = (d_3/d_1) = +1$, $(d_1/d_2)_4 \, (d_2/d_1)_4 = (d_2/d_3)_4 \, (d_3/d_2)_4 = (d_1/d_3)_4 \, (d_3/d_1)_4 = -1$, *and* $N\varepsilon = -1$.

Proof. First assume that $k^{(2)} = k^{(1)}$; Proposition 8 shows that k has a fundamental unit ε with norm -1. Moreover, if $(d_i/d_j) = +1$ for some i, j then the quadratic subfield $k_{ij} = \mathbb{Q}(\sqrt{d_i d_j})$ of k_{gen} must have class number $\equiv 2 \bmod 4$ (Corollary 1), and we deduce from Proposition 1 that $(d_i/d_j)_4 \, (d_j/d_i)_4 = -1$. This shows that the conditions in parts 2.–4. are necessary.

To prove their sufficiency, we apply the class number formula of Proposition 5 to $K = \mathbb{Q}(\sqrt{d_3}, \sqrt{d_1 d_2})$. We find $h_2(K) = (1/4) \, q(K) \, h_2(k_3) \, h_2(k_{12}) \, h_2(k) = (1/2) \, q(K) \, h_2(k)$ where $k_3 = \mathbb{Q}(\sqrt{d_3})$. Since ε_3 (the fundamental unit of k_3) and ε have norm -1, the only unit which could possibly become a square in K is ε_{12} (because such units must be totally positive); but by Proposition 3, $\delta(\varepsilon_{12}) = p_1$ (the prime dividing d_1; in fact, $(p_1, \sqrt{d_1 d_2})$ and $(p_2, \sqrt{d_1 d_2})$ are the only primitive ramified ideals different from (1) and $(\sqrt{p_1} \, \sqrt{p_2}))$, i.e. $k(\sqrt{\varepsilon}) = k(\sqrt{d_1}) \neq K$. Therefore we have $q(K) = 1$, which implies that $h_2(K) = \frac{1}{2} h_2(k)$; in particular, the class field tower terminates at $k^{(1)}$ by Proposition 7. This establishes parts 2, 3, 4 of the theorem.

We now consider the case $(d_1/d_2) = (d_2/d_3) = (d_3/d_1) = -1$. Then Proposition 2 shows that k admits a quaternion extension L/k which is unramified outside ∞; clearly $k^{(2)} = k^{(1)}$ implies that L is not real. Let ε_{ij} denote the fundamental unit of $\mathbb{Q}(\sqrt{d_i d_j})$. Our assumptions imply that $N\varepsilon_{ij} = -1$. Since L is real if and only if (2) is satisfied, the conditions given in part 1 are necessary. In order to prove that they are sufficient, we first observe that $\mathrm{Cl}_2(k) \simeq (2, 2)$. Therefore $k^{(2)} \neq k^{(1)}$ would imply the existence of an unramified normal extension L/k with $\mathrm{Gal}(L/k) \simeq D_4$ or $\mathrm{Gal}(L/k) \simeq H_8$ (cf. [11]). But by Propositions 1 and 2, such extensions do not exist in this case. ∎

Case 2. d is not a Sum of Two Squares.

Again we may assume that k is a real quadratic number field such that $\mathrm{Cl}_2(k)$ has rank 2, i.e. that $d = \operatorname{disc} k = d_1 d_2 d_3 d_4$ is the product of four prime discriminants, not all of them positive. Let p_j be the prime dividing d_j, for $j = 1, 2, 3, 4$.

THEOREM 2. *Let k be a real quadratic number field whose discriminant $d=d_1d_2d_3d_4$ is the product of four prime discriminants, not all of which are positive. Let δ be the square-free kernel of $N_{k/\mathbb{Q}}(\varepsilon+1)$ where ε is the fundamental unit of k. Then the 2-class field tower of k terminates at $k^{(1)}$ if and only if, after a suitable permutation of the indices, the d_i have the following properties*:

1. *all the d_i are negative*; *or*
2. $d_1, d_2>0$, *and*

(a) $(d_1/d_2)=(d_1/p_3)=(d_2/p_4)=-1$, $(d_1/p_4)=+1$; *or*

(b) $d_3d_4 \not\equiv 4 \bmod 8$, $(d_1/p_i)=(d_2/p_j)=-1$ $(i=2, 3, 4,\ j=1, 3, 4)$, *and* $\delta \neq p_1p_2$; *or*

(c) $d_4=-4$, $(d_1/d_2)=-1$, $d_1 \equiv d_2 \equiv 5 \bmod 8$, $(d_1/d_3)=(d_2/d_3)=+1$, *and* $\delta \neq p_1p_2$.

The proof of this theorem will be carried out in a number of stages below. First of all, suppose that all the d_i are negative; put $K=k(\sqrt{d_1d_2})$. We have to show that $h_2(K)=\frac{1}{2}h_2(k)$. By the class number formula, we find $h_2(K)=\frac{1}{4}q(K)\,h_2(k)$, since the subfields $\mathbb{Q}(\sqrt{d_1d_2})$ and $\mathbb{Q}(\sqrt{d_3d_4})$ have odd class number by genus theory. Let ε_{ij} denote the positive fundamental unit of $\mathbb{Q}(\sqrt{d_id_j})$; if we had $4 \mid q(K)$, then at least one of the units ε_{12}, ε_{34} or $\varepsilon_{12}\varepsilon_{34}$ must become a square in K. But since $\delta(\varepsilon_{12})=p_1$ and $\delta(\varepsilon_{34})=p_3$ or perhaps $2p_3$ (without loss of generality), Proposition 3 shows that $\sqrt{\varepsilon_{12}}$, $\sqrt{\varepsilon_{34}}$ and $\sqrt{\varepsilon_{12}\varepsilon_{34}}$ are not in K. This shows that $q(K) \mid 2$; since $\frac{1}{2}h_2(k) \mid h_2(K)$, the class number formula now shows that $q(K)=2$ and $h_2(K)=\frac{1}{2}h_2(k)$ as claimed.

Now assume that exactly two of the d_i, say d_3 and d_4, are negative. We first show

PROPOSITION 9. *Let the assumptions of Theorem 2 be satisfied, and suppose in addition that $d_1, d_2>0$ and $d_3, d_3<0$. Put $F=\mathbb{Q}(\sqrt{d_1d_2})$ and $K=kF$. Then k has abelian 2-class field tower if and only if $(d_1/d_2)=-1$ and $q(K)=1$.*

Proof. Assume first that $(d_1/d_2)=-1$ and $q(K)=1$. The class number formula for K shows that

$$h_2(K)=\tfrac{1}{4}q(K)\,h_2(F)\,h_2(k); \tag{3}$$

if $(d_1/d_2)=-1$ then $h_2(F)=2$, and $q(K)=1$ now gives $h_2(K)=\frac{1}{2}h_2(k)$. Thus by Proposition 7 we conclude that k has abelian 2-class field tower in this case.

For the proof of the converse, assume that the 2-class field tower of k is abelian. If we had $(d_1/d_2) = +1$, then F would possess a cyclic quartic extension $L = F(\sqrt{d_1}, \sqrt{\alpha})$ (for some $\alpha \in \mathbb{Q}(\sqrt{d_1})$) which is unramified at the finite primes and has dihedral Galois group over $\mathbb{Q}$. In particular, L is either totally real or totally complex. In the first case, $k(\sqrt{d_3 d_4}, \sqrt{\alpha})/k$ is a dihedral extension of k which is unramified everywhere, in the second case $k(\sqrt{d_3 d_4}, \sqrt{d_3 \alpha})/k$ is such an extension. Thus we must have $(d_1/d_2) = -1$ as claimed. Now $q(K) = 1$ follows from (3) and the converse direction of Proposition 7. ▮

Let us continue with the proof of Theorem 2. We assume that k has abelian 2-class field tower. The preceding proposition shows that $(d_1/d_2) = -1$.

LEMMA. *If* $(d_1/p_3) = (d_1/p_4) = +1$, *then* $k^{(1)} \neq k^{(2)}$.

This is easy to see: in this case, $F = \mathbb{Q}(\sqrt{d_1 d_3 d_4})$ has a cyclic quartic extension $L = F(\sqrt{d_1}, \sqrt{\alpha})$ for some $\alpha \in \mathbb{Q}(\sqrt{d_1})$ which is unramified outside ∞ and normal over $\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \simeq D_4$ (see [17]). But then either $k(\sqrt{d_2}, \sqrt{\alpha})$ or $k(\sqrt{d_2}, \sqrt{d_3 \alpha})$ is a D_4-extension of k which is unramified everywhere.

Thus we may assume that at least one of (d_1/p_3) or (d_1/p_4) is negative; exchanging d_3 and d_4 if necessary we may assume that $(d_1/p_3) = -1$. Now we distinguish two cases:

(A) $(d_1/p_4) = +1$.

Suppose, first of all, that $d \not\equiv 4 \bmod 8$. Then we claim that $(d_2/p_4) = -1$. For, if $(d_2/p_4) = +1$, then either $(d_2/p_3) = +1$ (and the preceding Lemma with d_1 replaced by d_2 shows that k has an unramified dihedral extension), or $(d_2/p_3) = -1$; in this case, $(d_1 d_2/p_3) = (d_1 d_2/p_4) = (d_2 d_3 d_4/p_1) = (d_1 d_3 d_4/p_2) = +1$ by quadratic reciprocity. But then (apply Proposition 2 to the factorization $d_1 \cdot d_2 \cdot d_3 d_4$) there exists a quaternion extension of k which is unramified outside ∞ and normal over $\mathbb{Q}$; by twisting the extension with $\sqrt{d_3}$ if necessary (that is, replacing $k(\sqrt{d_1}, \sqrt{d_2}, \sqrt{\alpha})$ by $k(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3 \alpha})$) we can make it unramified everywhere: a contradiction. This establishes 2.(a) of Theorem 2.

On the other hand, suppose $d \equiv 4 \bmod 8$. If $d_4 = -4$, then the previous argument again establishes 2.(a). Now suppose $d_3 = -4$ and that $(d_2/p_4) = +1$. Then $\delta \neq p_1 p_2$ (otherwise $\sqrt{\varepsilon} \in K = k(\sqrt{d_1 d_2})$, which would imply that $2 \mid q(K)$, contradicting the assumption that $k^{(1)} = k^{(2)}$ by Proposition 9). This establishes 2.(c) of the theorem.

(B) $(d_1/p_4) = -1$.

As in case A, $(d_2/p_3) = -1$ or $(d_2/p_4) = -1$. If $(d_2/p_3)(d_2/p_4) = -1$, then 2.(a) of the theorem follows. So assume that $(d_2/p_3) = (d_2/p_4) = -1$. If $d \not\equiv 4 \bmod 8$, then $\delta \neq p_1 p_2$ by Proposition 3; this establishes 2.(b) in this case. If, on the other hand, $d \equiv 4 \bmod 8$, say $d_4 = -4$, then $d = d_1 \cdot d_2 \cdot d_3 d_4$ satisfies the conditions of Proposition 2; thus there exists an unramified H_8-extension (we may have to twist it with $\sqrt{d_3}$ in order to make it unramified at ∞), and we see that $k^{(1)} \neq k^{(2)}$. Hence this last assumption is vacuous.

All of this establishes that in 2. of Theorem 2, if $k^{(1)} = k^{(2)}$, then one of the statements (a), (b), or (c) holds.

Now we consider the converse to the previous statement. Let k satisfy the assumptions of Theorem 2. We consider three cases.

(a) $(d_1/d_2) = (d_1/p_3) = (d_2/p_4) = -1$, $(d_1/p_4) = +1$:

Then Propositions 1 and 2 of [2] show that $\mathrm{Cl}_2(k) \simeq (2.2)$. But then $k^{(1)} = k^{(2)}$, by Theorem 2 of [2].

(b) $d_3 d_4 \not\equiv 4 \bmod 8$, $(d_1/d_i) = (d_2/d_j) = -1$ $(i = 2, 3, 4,\ j = 1, 3, 4)$, and $\delta \neq p_1 p_2$.

By Proposition 9, we need to show that $q(K) = 1$. To this end, first notice that $q(K) = (E_K : E_k E_{k_{12}} E_{k_{34}}) = (E_K : \langle -1, \varepsilon, \varepsilon_{12}, \varepsilon_{34} \rangle)$. Since $N\varepsilon_{12} = -1$, the only possible products of the fundamental units which could become squares in K are ε, ε_{34}, and $\varepsilon\varepsilon_{34}$ (since these are—modulo squares—the only totally positive units in K). We now show that none of these units is a square in K. Let $\delta_{34} = \delta(\varepsilon_{34})$. By Proposition 3, we have (because of our assumptions in this case) that $\delta \in \{p_1 p_3, p_1 p_4\}$ and $\delta_{34} = p_3$. Notice then that δ, δ_{34}, and $\delta\delta_{34}$ are not squares in K. Hence Proposition 3 shows that $\sqrt{\varepsilon}$, $\sqrt{\varepsilon_{34}}$, $\sqrt{\varepsilon\varepsilon_{34}}$ are not in K. Thus $q(K) = 1$. By Proposition 9, we conclude that $k^{(1)} = k^{(2)}$.

(c) $d_4 = -4$, $(d_1/d_2) = -1$, $d_1 \equiv d_2 \equiv 5 \bmod 8$, $(d_1/d_3) = (d_2/d_3) = +1$, and $\delta \neq p_1 p_2$:

The proof is the same as the previous case except that $\delta = 2p_1 p_3$ and $\delta_{34} \in \{2, 2p_3\}$, which again implies that $q(K) = 1$. Thus $k^{(1)} = k^{(2)}$.

Theorem 2 is now established.

4. SOME REMARKS ON UNITS

The following byproducts of our proofs complement Dirichlet's results [4] on the norms of units in quadratic number fields:

COROLLARY 3. *Let d_1, d_2, d_3 be prime discriminants such that $(d_1/d_2) = (d_2/d_3) = 1$ and $(d_3/d_1) = -1$, and let ε denote the fundamental unit of $\mathbb{Q}(\sqrt{d_1 d_2 d_3})$. Then*

$$N\varepsilon = -1 \Rightarrow \left(\frac{d_1}{d_2}\right)_4 \left(\frac{d_2}{d_1}\right)_4 = \left(\frac{d_2}{d_3}\right)_4 \left(\frac{d_3}{d_2}\right)_4.$$

Proof. Suppose that $N\varepsilon = -1$ (note that this implies $d_j > 0$) and $(d_1/d_2)_4 \, (d_2/d_1)_4 = -1$. In the proof of Theorem 1 we have shown that this implies that $h_2(K) = \frac{1}{2} h_2(k)$ where $K = \mathbb{Q}(\sqrt{d_3}, \sqrt{d_1 d_2})$.

Therefore, the 2-class field tower of k terminates at $k^{(1)}$, hence the subfield $L = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2 d_3})$ must also have 2-class number $h_2(L) = \frac{1}{2} h_2(k)$. This in turn implies that $(d_2/d_3)_4 \, (d_3/d_2)_4 = -1$.

Similarly, $(d_1/d_2)_4 \, (d_2/d_1)_4 = +1$ implies that $(d_2/d_3)_4 \, (d_3/d_2)_4 = +1$. ∎

COROLLARY 4. *Let d_1, d_2, d_3 be prime discriminants such that $(d_1/d_2) = (d_2/d_3) = (d_3/d_1) = +1$, and let ε denote the fundamental unit of $\mathbb{Q}(\sqrt{d_1 d_2 d_3})$. Then*

$$N\varepsilon = -1 \Rightarrow \left(\frac{d_1}{d_2}\right)_4 \left(\frac{d_2}{d_1}\right)_4 = \left(\frac{d_2}{d_3}\right)_4 \left(\frac{d_3}{d_2}\right)_4 = \left(\frac{d_1}{d_3}\right)_4 \left(\frac{d_4}{d_1}\right)_4.$$

Proof. This is proved similarly. ∎

We were not able to replace the conditions on δ in Theorem 2 by conditions on power residue symbols. Observe, however, the following result:

PROPOSITION 10. *Assume the notation of Theorem* 2.2(b); *then $\delta = p_1 p_2$ implies*

$$\left(\frac{d_3 d_4}{d_1}\right)_4 = \left(\frac{d_3 d_4}{d_2}\right)_4. \tag{4}$$

Proof. We only treat the case $d \equiv 1 \bmod 4$, the other cases being similar. From Proposition 3 we know that $\delta = p_1 p_2$ if and only if there is a principal ideal of norm $p_1 p_2$. This implies that $\pm 4 p_1 p_2 = A^2 - mB^2$ has solutions, where m is squarefree such that $k = \mathbb{Q}(\sqrt{m})$. Raising this equation to the third power we get $\pm (p_1 p_2)^3 = X^2 - my^2$. Clearly $X = p_1 p_2 x_1$; this gives $\pm 1 = p_1 p_2 x^2 - p_3 p_4 y^2$. Reducing the equation modulo p_3 and observing that $(p_1 p_2 / p_3) = +1$ by assumption we find that the plus sign must hold:

$$p_1 p_2 x^2 - p_3 p_4 y^2 = 1. \tag{5}$$

Reducing this equation modulo p_1 and p_2, we get $(-p_3p_4/p_1)_4(y/p_1)=1$ and $(-p_3p_4/p_2)_4(y/p_2)=1$, respectively. Write $y=2^ju$ with $u\equiv 1 \bmod 2$; then $(p_1p_2/u)=+1$, hence $(y/p_1p_2)=(2/p_1p_2)^j(p_1p_2/u)$. Now $(2/p_1p_2)^j=(2/p_1p_2)$ gives

$$1=\left(\frac{-p_3p_4}{p_1p_2}\right)\left(\frac{y}{p_1p_2}\right)=\left(\frac{-p_3p_4}{p_1p_2}\right)\left(\frac{2}{p_1p_2}\right).$$

But $(-1/p_1p_2)_4=(2/p_1p_2)$, and our claim follows. ∎

The very same result holds in case 2.2(c); but here things simplify, because $d_1\equiv d_2\equiv 5 \bmod 8$ implies that $(-4/d_j)=(-1/d_j)_4(2/d_j)=+1$ for $j=1,2$. The proof of the following proposition is left to the reader:

Proposition 11. *Assume the notation of Theorem* 2.2(c), *then* $\delta=p_1p_2$ *implies*

$$\left(\frac{d_3}{d_1}\right)_4=\left(\frac{d_3}{d_2}\right)_4.$$

ACKNOWLEDGMENT

We thank the referees for their careful reading of the manuscript and for their helpful comments.

REFERENCES

1. E. Benjamin, F. Sanborn, and C. Snyder, Capitulation in unramified quadratic extensions of real quadratic number fields, *Glasgow Math. J.* **36** (1994), 385–392.
2. E. Benjamin and C. Snyder, Real quadratic number fields with 2-class group of type (2, 2), *Math. Scand.* **76** (1995), 161–178.
3. R. J. Bond, Unramified abelian extensions of number fields, *J. Number Theory* **30** (1980), 1–10.
4. L. Dirichlet, Einige neue Sätze über unbestimmte Gleichungen, *in* "Gesammelten Werke," pp. 219–236, Birkhäuser, Basel.
5. A. Fröhlich, "Central Extensions, Galois Groups, and Ideal Class Groups of Number Fields," Contemp. Math., Vol. 24, Amer. Math. Soc., Providence, 1983.
6. Y. Furuta, Über das Verhalten der Ideale des Grundkörpers im Klassenkörper, *J. Number Theory* **3** (1971), 318–322.
7. E. S. Golod and I. R. Shafarevic, Infinite class field towers of quadratic fields, *Izv. Akad. Nauk. SSSR* **28** (1964), 273–276 [In Russian]; English translation, *Amer. Math. Soc. Transl.* **48** (1965), 91–102.
8. K. Iwasawa, A note on the group of units of an algebraic number field, *J. Math. Pures Appl.* **35** (1956), 189–192.
9. P. Kaplan, Sur le 2-groupe des classes d'idéaux des corps quadratiques, *J. Reine Angew. Math.* **283/284** (1974), 313–363.

10. G. Karpilovsky, "Schur Multipliers," London Math. Soc. Monographs, Oxford Univ. Press, London, 1987.
11. H. Kisilevsky, Number fields with class number congruent to 4 mod 8 and Hilbert's theorem 94, *J. Number Theory* **8** (1976), 271–279.
12. T. Kubota, Über den Bizyklischen Biquadratischen Zahlkörper, *Nagoya Math. J.* **10** (1956), 65–85.
13. H. Kurzweil, "Endliche Gruppen," Springer-Verlag, Heidelberg, 1977.
14. F. Lemmermeyer, Unramified quaternion extensions of quadratic number fields, *J. Théor. Nombres Bordeaux* **9** (1997), 51–68.
15. J. Martinet, Tours de corps de classes et estimations de discriminants, *Invent. Math.* **44** (1978), 65–73.
16. P. Morton, Density results for the 2-class groups and fundamental units of real quadratic fields, *Studia Sci. Math. Hungar.* **17** (1982), 21–43.
17. L. Rédei and H. Reichardt, Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, *J. Reine Angew. Math.* **170** (1934), 69–74.
18. A. Scholz, Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$, *Math. Z.* **39** (1934), 95–111.
19. R. Schoof, Infinite class field towers of quadratic fields, *J. Reine Angew. Math.* **372** (1986), 209–220.
20. S. Shirai, Central class numbers in central class field towers, *Proc. Japan Acad.* **51** (1975), 389–393.
21. D. B. Zagier, "Zetafunktionen und quadratische Körper," Springer-Verlag, New York/Berlin, 1981.